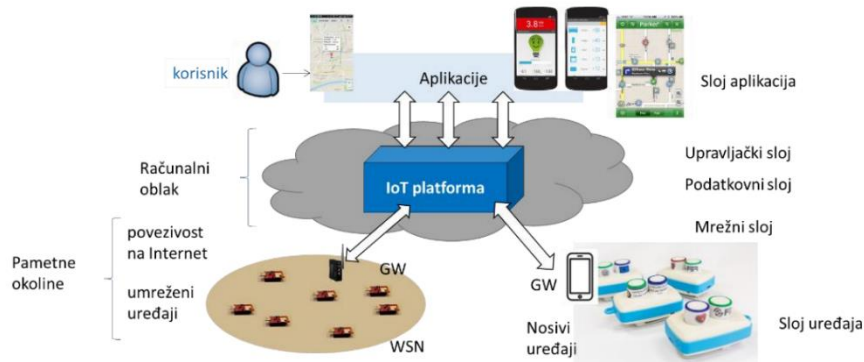


2. prezentacija

INTERNET STVARI

- Pojednostavljena arhitektura IoT-a



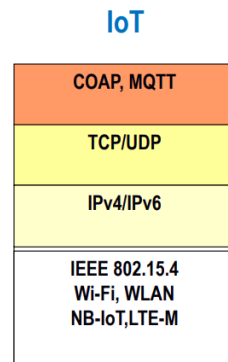
- Komponente sustava:
 - Nosivi uređaji, WSN (sloj uređaja)** – prikupljaju podatke o okolini (senzori) ili izvršavaju određene funkcije (aktuatori)
 - Mrežni sloj** – omogućuje komunikaciju između IoT-uređaja i računalnog oblaka za pohranu podataka
 - Računalni oblak (podatkovni i upravljački sloj)** – pohranjuje podatke prikupljenje sa IoT-uređaja, izvršava analizu podataka, omogućuje upravljanje IoT-uređajima
 - Aplikacije (aplikacijski sloj)** – omogućuju prikaz podataka krajnjim korisnicima
- Mrežna infrastruktura temeljena na protokolu IP:
 - Nepokretne mreže**
 - Pokretne mreže**
 - Bežične mreže**
 - Osobne mreže**

SLOJ UREĐAJA

- **IoT uređaj (senzorski čvor)**
 - uređaj za opažanje fenomena iz okoline, malih je dimenzija, troši malo energije te posjeduje ograničene resurse
 - podatke šalje bežično do sljedećeg senzora ili do usmjeritelja (engl. gateway, GW) koji je povezan na Internet, nastaje bežična senzorska mreža (engl. Wireless Sensor Network, WSN)
 - sastoji se od komponenti za opažanje i mjerenje fenomena iz okoline, procesora i memorije te komponente za komunikaciju
- **Aktuator**
 - uređaj koji u kombinaciji sa sensorima, na temelju očitavanja iz okoline, izvodi određenu akciju u okolini
- **Obilježja hardvera**
 - male dimenzije, mala potrošnja, niska cijena, umrežavanje na načelu samoorganizacije
- **Mikroprocesori i mikrokontroleri**
 - na jednom chipu imaju integriran RAM, ROM i internu sabirnicu

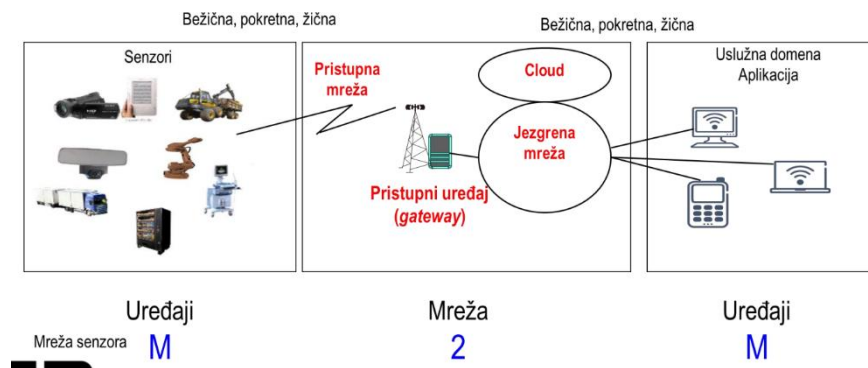
SLOJ PODATKOVNE POVEZNICE: M2M-KOMUNIKACIJA

- **Protokolni složaj za IoT**



- **Bežična mreža senzora (WSN)**
 - čini ju skup senzora, na nekom zemljopisnom području, koji međusobno surađuju
 - senzori detektirane podatke šalju do posebnog čvora
 - RAZLIKE U ODNOSU NA AD HOC:
 - broj senzora je puno veći i senzori su postavljeni gusto
 - senzori su skloni ispadima
 - topologija mreže je stabilnija
 - ograničeni resursi

- Vrste mreža senzora:
 - Kopnena mreža senzora
 - Podzemna mreža senzora
 - Podvodna mreža senzora
 - Višemedijska mreža senzora
 - Pokretna mreža senzora
- **Machine-to-Machine**
 - mreža koja omogućava komunikaciju krajnjih uređaja
 - računalni sustav koji upravlja drugim uređajima



- jezgrena mreža – veza s korisnikom, internetska mreža, uslužne aplikacije
- pristupni uređaj – povezuje pristupnu i jezgrena mrežu

3. prezentacija

KOMUNIKACIJA UREĐAJA

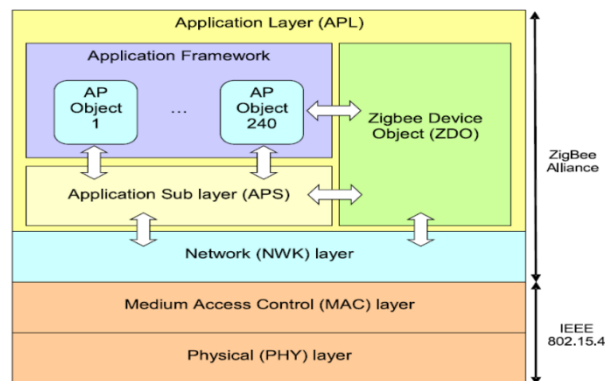
- **Zahtjevi:**
 - što veći domet
 - mala potrošnja
 - niska cijena
 - jednostavno uvođenje u sustav
 - malo kašnjenje
 - podrška za masovnu primjenu
- **Domet:**
 - Kratki
 - Bluetooth
 - 802.15.7 VLC
 - Srednji
 - ZigBee
 - IEEE 802.15.4 XBee
 - IEEE 802.11 Wi-Fi
 - Z-wave
 - IEEE 802.3 Ethernet
 - Dugi
 - 2G – 5G (NB-IoT)
 - LoRaWAN, Sigfox
- **Frekvencijski spektar:**
 - Nelicencirani spektar (2.4 GHz)
 - Prednosti: lakše postavljanje, veći kapacitet
 - Nedostaci: interferencija, zatvoreni prostor smanjuje domet, veća potrošnja
 - Spektar sa frekvencijama ispod 1 GHz
 - Prednosti: veći domet, prolazi kroz zidove, manja potrošnja
 - Nedostaci: manji kapacitet, dozvola za neke
 - 169 MHz, 422 MHz, 868 Mhz, 915 Mhz, 779-787 MHz
- **Potrošnja energije**
 - Klase:
 - **Ograničenje događajem** - skupljanje energije iz događaja
 - **Ograničenje vremenskim** periodom - periodička zamjena ili punjenje
 - **Ograničenje životnim vijekom** - nema zamjenjivih baterija
 - **Bez ograničenja** - priključeno na napajanje
 - Smanjenje potrošnje – isključenje pojedinih dijelova uređaja za vrijeme rada, koriste se bežične komunikacije koje manje troše, optimizirane komponente

- **Strategije korištenja energije za komunikaciju:**
 - Normalno je isključeno - ponovno spajanje po potrebi.
 - Niska potrošnja - periodičko isključivanje
 - Uvijek uključeno - cijelo vrijeme može komunicirati
- **Topologije:**
 - zvijezda (WiFi)
 - peer-to-peer
 - stablo
 - mesh (IEEE 802.15.4)
- IEEE 802.15.
 - standard koji specificira bežične tehnologije prijenosa podataka s niskom potrošnjom i ograničenim mogućnostima
 - Zigbee, 6LoWPAN, Thread, ZigBee IP ga koriste
 - **Klase uređaja:**
 - Full-function device (FFD)
 - podržava sve mogućnosti
 - može primati, slati i usmjeravati pakete
 - koordinator, usmjeritelji moraju biti FFD
 - Reduced-function device (RFD)
 - ograničene mogućnosti
 - krajnji čvor u mreži (može biti RFD ili FFD)
 - mala potrošnja, mogućnost sleep-a
 - može komunicirati samo s FFD-ovima
 - **Način rada:**
 - Beacon-mode
 - koordinator upravlja i sinkronizira prijenos podataka
 - svi ostali čvorovi osluškuju beacon
 - omogućuje duty-cycling (čvorovi mogu ući u sleep radi potrošnje)
 - Non-beacon mode
 - za komunikaciju od točke do točke
 - čvorovi moraju kontinuirano osluškivati stanje u kanalu
 - enkripcijski algoritam (AES)

ZIGBEE

- za primjene koje zahtijevaju malu brzinu, nisku potrošnju, malo kašnjenje i sigurnu komunikaciju
- mreža otporna na kvarove i robusna, mesh topologija
- **Protokolni sadržaj**
 - **NWK (Network layer)**
 - omogućuje sigurno višeskokovno usmjeravanje, otkrivanje i održavanje puteva, ulazak i napuštanje mreže, dodjeljivanje adresa novim čvorovima

- Funkcije:
 - pokretanje mreže
 - priključivanje i napuštanje mreže
 - konfiguracija
 - adresiranje
 - sinkronizacija
 - sigurnost
 - usmjeravanje
- **APL (Application Layer)**
 - predstavlja okvir za razvoj raspodjeljenih aplikacija i komunikaciju
- **ZDO (Zigbee Device Object)**
 - omogućava međusobno otkrivanje APO-a i njihovu organizaciju u raspodjeljenu aplikaciju



- **AODV usmjeravanje (Ad Hoc On-Demand Distance Vector Routing)**
 - održava tablice usmjeravanja na putu među čvorovima koji žele komunicirati
 - preplavljuje porukama route request da bi se otkrio put do odredišta
- Funkcije aplikacijskog sloja (ZIGBEE)
 - ZDO održava što koji uređaj može što raditi i obrađuje zahtjeve za povezivanje
 - klasteri, endpoint, otkrivanje, povezivanje
- Temelji se na AES-u
- **Trust centar** – čvor zadužen za sigurnost
 - Trust Manager - autentifikacija uređaja koji se žele priključiti mreži
 - Network Manager – održava i distribuira mrežne ključeve
 - Configuration Manager – omogućuje sigurnost s kraja na kraj između uređaja
- Zigbee ključevi
 - Master ključevi
 - koriste se za inicijalnu razmjenu tajni između dva uređaja

- Mrežni ključevi
 - osiguravaju mrežu
- Ključevi poveznice
 - osiguravaju poruke na aplikacijskoj razini

Z-WAVE

- stablasta topologija mreže
- za razliku od Zigbee-ja ima samo dvije frekvencije 868 Mhz i 908 MHz
- koristi svoj protocol za razliku od Zigbee-ja koji koristi IEEE 802.15.4 protokol
- ima veći doseg od Zigbee-ja zbog nižih frekvencija na kojima radi
- načini slanja:
 - single
 - multicast
 - broadcast

IEEE 802.11AH

- varijanta WiFi-ja
- predviđen za IoT uređaje, troši malo energije
- domet: 1km, max. brzina: 100kb/s
- 3 područja primjene:
 - Senzori i brojila
 - Agregacija podataka iz industrijskih postrojenja
 - Proširivanje WiFi-ja na otvorenom prostoru
- koristi nelicencirana područja <1 GHz
- koristi modulaciju OFDM
- **Restricted access window (RAW)** - algoritam za izbjegavanje istovremenog slanja paketa
- **Target wake time (TWT)** – AP može definirati kada se uređaj može spojiti, uređaj može u međuvremenu „spavati”

4. prezentacija

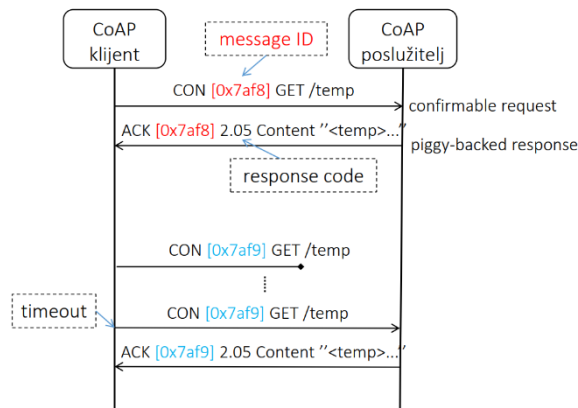
CONSTRAINED APPLICATION PROTOCOL (COAP)

- **CoAP framework** – definira jednostavne i fleksibilne načine za slanje i primanje podataka s IoT uređaja
- resursi se identificiraju pomoću URI-ja, IoT uređaj postaje poslužitelj koji nudi resurse
- klijenti pristupaju resursima pomoću asinkronog mehanizma zahtjev-odgovor
- koristi UDP kao transportni protocol
- koristi tehnike za kompresiju podataka
- sigurna komunikacija omogućena protokolnom DTLS
- **Vrste CoAP poruka:**
 - Confirmable Message
 - Non-Confirmable Message
 - Acknowledgement Message
 - Reset Message
- **Metode CoAP-a**
 - GET
 - POST
 - PUT
 - DELETE
- **Prijenos poruka**
 - poruka nosi zahtjev, odgovor ili je prazna
 - poruke se razmjenjuju asinkrono
- **Prednosti:**
 - prilagođen uređajima i mrežama ograničenih resursa
 - mala potrošnja
 - temelji se na REST-u
 - omogućuje potvrdu poruke
 - DTSL se koristi za šifriranje poruka
- **Nedostaci:**
 - komunikacija je uvijek 1 na 1
- **Zaglavlje CoAP poruke**

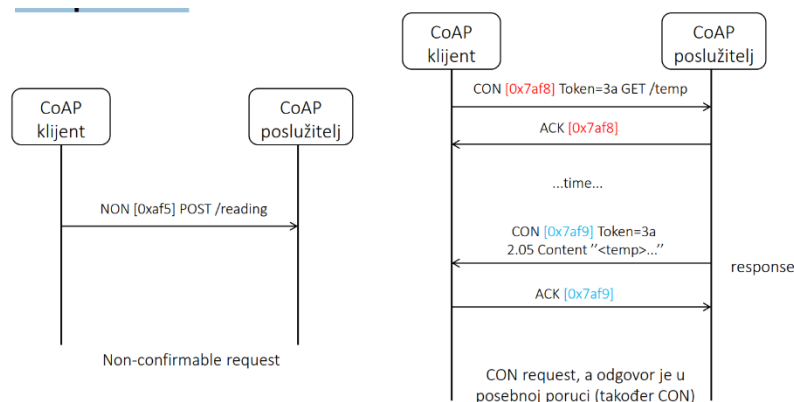
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Ver		T		TKL					Code								Message ID														
Token + Options (if any)																															
1	1	1	1	1	1	1	1	1	Payload (if any)																						

- **Version (Ver)** – verzija CoAP protokola

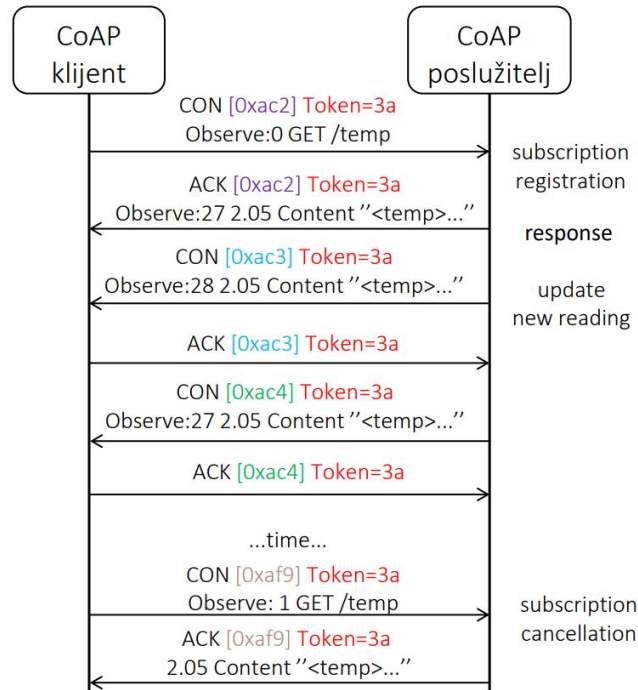
- **Type (T)** – predstavlja jedan od tipova poruka
- **Token Length (TKL)** – predstavlja duljinu polja Token
- **Code** – 8-bitni prirodni broj
 - **klase:**
 - Request
 - Success response
 - Client error message
 - Server error response
 - Empty message
- **Message ID** - za detekciju višestrukih poruka i povezivanje poruka tipa Acknowledgement/Reset s porukama tipa Confirmable/Non-confirmable
- **Token** – koristi se za povezivanje zahtjeva i njegovog odgovora te je neovisan o Message ID
- **Razmjena poruka:**
 - **Confirmable request**



- **Non-confirmable request i separate response**



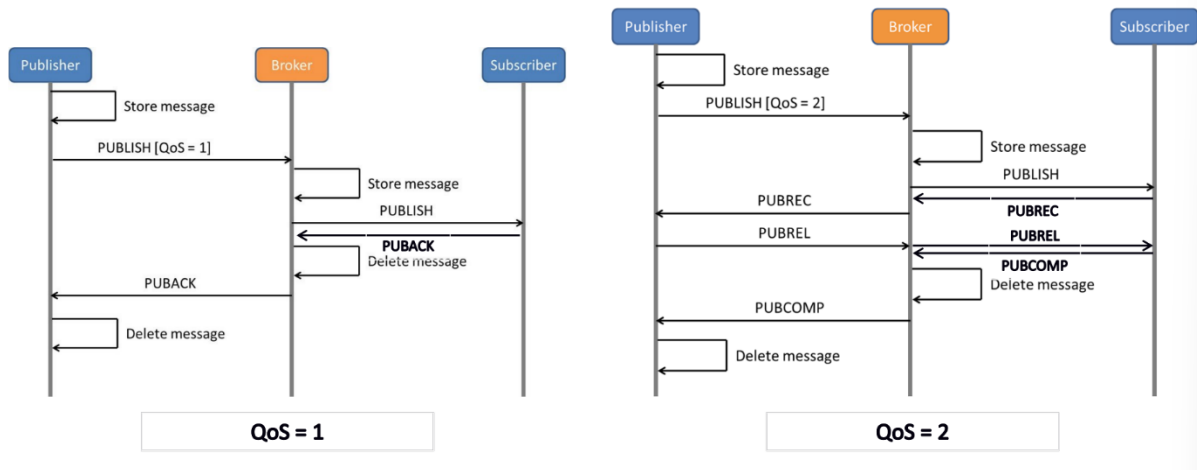
- **Observation**



MESSAGE QUEUING TELEMETRY TRANSPORT (MQTT)

- jednostavan protokol za prijenos poruka na načelu publish-subscribe prilagođen uređajima i mrežama s ograničenim resursima
- koristi TCP/IP na mrežnom sloju
- **Osnovni komunikacijski mehanizam**
 - MQTT Broker - posrednik između publishera i subscibera
 - MQTT Client
 - Publisher - objavljuje poruke na Topic
 - Subscriber – pretplaćuje se na ena Topic, prima objavljene poruke
- **Kontrolni paketi**
 - sastoje se od varijabilnog zaglavlja i sadržaja
 - MQTT prenosi kontrolne pakete putem TCP-a
 - TCP osigurava ispravan prijenos paketa bez gubitaka
- **MQTT – sjednica**

PUBLISH, QoS>0



- **Prednosti:**
 - prilagođen uređajima i mrežama ograničenih resursa
 - pouzdana isporuka poruka
 - pretplata omogućuje isporuke na više odredišta
- **Nedostaci:**
 - korištenje TCP-a dodaje značajni overhead
 - značajna potrošnja na IoT uređajima, nepogodan za uređaje s ograničenom količinom energije
- **CoAP vs MQTT**

	CoAP	MQTT
Communications Model	Request-Response, or Pub-Sub	Pub-Sub
RESTful	Yes	No
Transport Layer Protocol	Preferably UDP; TCP can be used	Preferably TCP; UDP can be used (MQTT-S)
Header	4 Bytes	2 Bytes
Number of message types	4	16
Messaging	Asynchronous and Synchronous	Asynchronous
Application Reliability	2 Levels	3 Levels
Security	IPSEC or DTLS	TLS
Intermediaries	Yes	Yes (MQTT-S)

5. prezentacija

LOW POWER WIDE AREA NETWORK (LPWAN)

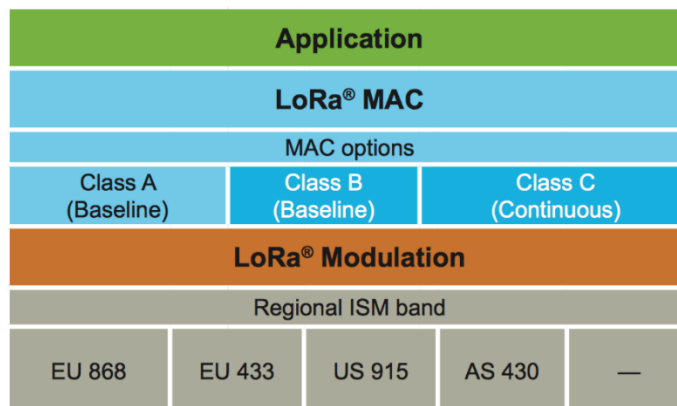
- mala potrošnja energije
- uređaji mogu raditi na bateriju
- velike udaljenosti komunikacije
- niže frekvencije
- manja brzina prijenosa podataka

SIGFOX

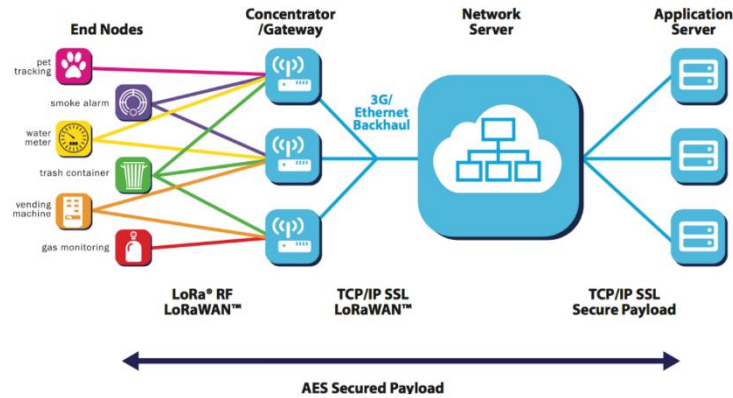
- koristi nelicencirani pojas ISM
- originalno je zamišljen da je komunikacija ide u jednom smjeru
- za slanje male količine podataka u burstevima
- Ograničenja
 - 140 poruka dnevno
 - 12 okteta slanje, 8 okteta primanje
 - brzina slanja 100bps, brzina primanja 600bps
- Fizički sloj
 - Ultra Narrow Band
 - Frekvencije 868 MHz i 902 MHz
 - 333 kanala

LoRa i LoRaWAN

- LoRa – definira fizički sloj
- LoRaWAN – definira protocol i arhitekturu sustava
- LoRa – arhitektura čvora:



- **LoRa – mrežna arhitektura:**



- **ChirpStack**

- LoRaWAN Network Server složaj otvorenog koda
- komponente:
 - ChirpStack Gateway Bridge – komunikacija s mrežnim prilazom
 - ChirpStack Network Server – implementacija mrežnog poslužitelja
 - ChirpStack Application Server – implementacija aplikacijskog poslužitelja
 - ChirpStack Gateway OS – za izvođenje cijelog složaja na mrežnom prilazu koji je na RPi-u

- **LoRa – klase uređaja**

- Klasa A
 - najbolje za napajanje baterijama
 - slanje podataka na uređaj moguće je samo nakon uspješnog slanja
 - koristi se mehanizam ALOHA
- Klasa B
 - primanje u raspoređenom vremenskom period
 - prima signal za sinkronizaciju od GW-a
- Klasa C
 - kontinuirano ima otvoreni prozor za primanje
 - primanje se zaustavlja jedino kada se šalju podaci

- **Sigurnost** – koristi se AES – 128

- **LoRaWAN aktivacija**

- potrebna aktivacija prije korištenja u mreži
- Informacije potrebne za aktivaciju:
 - adresa uređaja
 - ključ mrežne sjednice
 - ključ aplikacijske sjednice

- **Dvije aktivacijske metode:**
 - Over-the-Air Activation (OTA A)
 - temelji se na globalno jedinstvenom identifikatoru
 - poruku se razmjenjuju bežično
 - Activation By Personalization (ABP)
 - Dijeljeni ključevi se pohranjuju na krajnji uređaj u proizvodnji
 - Vrijede samo za specifičnu mrežu
- **Implementacije**
 - komercijalne – operatori pružaju mrežu i naplaćuju je
 - javne – bilo tko se može uključiti i pružati pristup
 - private – svatko može pokrenuti svoju privatnu mrežu

LTE-M

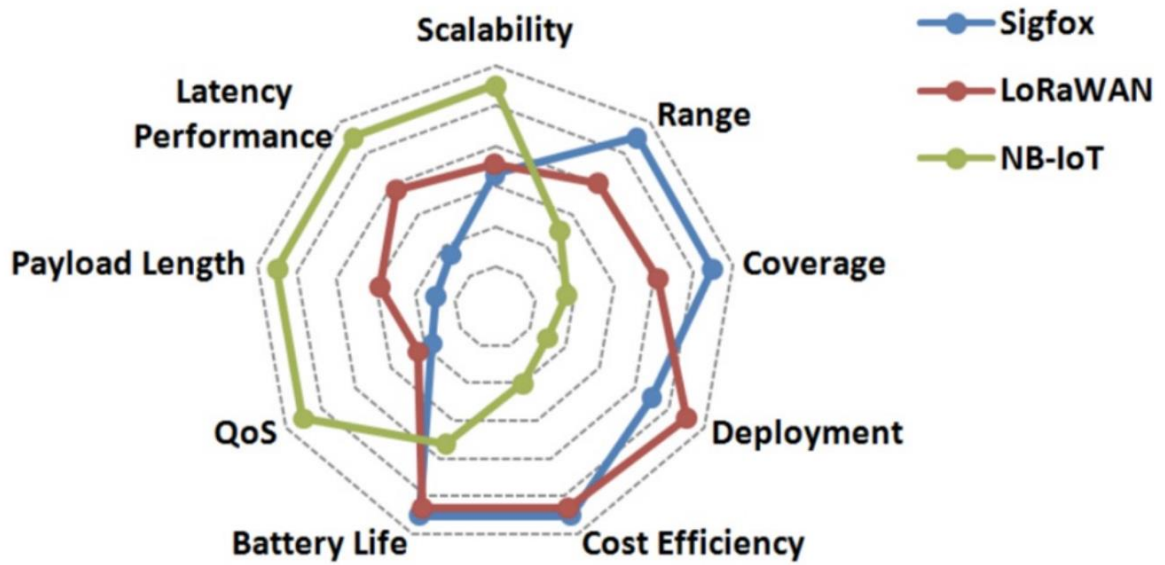
- LTE Cat 0
 - smanjene brzine prijenosa na 1 Mbps
 - Half-duplex komunikacija
 - Uveden Power Save Mode (PSM)
 - uređaj može ući u duboki san i brzo se probuditi i povezati
 - može se jednom dnevno buditi i slati podatke
 - maksimalni period spavanja 12.1 dana
- LTE Cat-1
 - koristi se najviše u SAD-u za M2M komunikaciju
 - veće brzine: 10/5 Mbps
 - može prenositi zvuk i video
- LTE Cat-M1
 - smanjena širina pojasa sa 20MHz na 1,4Mhz
 - smanjena izlazna snaga za 50%
 - brzine 375 Kbps ili 1 Mbps
 - primjena: V2V, zvuk
 - dodani mehanizmi za mogućnost kratkog spavanja uređaja (10,24s)

NB-IoT

- omogućuje uređajima povezivanje na internet preko postojećih mobilnih mreža
- nema prijenosa zvuka i videa
- širina kanala 180 kHz
- Smještaj kanala:
 - Između dva LTE kanala
 - Na mjestu GSM kanala

- Unutar LTE kanala

- Usporedba tehnologija:



6. prezentacija

UREĐAJI OGRANIČENIH RESURSA

- uređaji s ograničenom memorijom, procesorom, napajanjem
- smanjena sposobnost obrade podataka, mala veličina okvira pri prijenosu podataka
- Podjela:
 - **Uređaji kategorije 0**
 - imaju izrazito ograničene resurse, ne implementiraju IP stack i sigurnosne mehanizme
 - rijetko komuniciraju, prenose nekoliko byte-ova, ograničene sigurnosne i upravljačke mehanizme
 - **Uređaji kategorije 1**
 - ne implementiraju IP stack u cijelosti, podržavaju CoAP
 - imaju dovoljno resursa za implementaciju IP stack prilagođen hw za direktnu komunikaciju s poslužiteljem ili putem posrednika
 - **Uređaji kategorije 2**
 - implementiraju IP stack u cijelosti
 - resursi su usporedivi s resursima osobnog računala
 - podržavaju puni IP stack, ali treba voditi računa o ograničenjima pristupne tehnologije

MREŽA OGRANIČENIH RESURSA

- bežična mreža čvorova s ograničenim izvorom energije
- potencijalno dugi periodi neaktivnosti čvorova
- ograničena širina pojasa i propusnost
- nelicencirani spektar
- koriste tehnologije: star, mesh, P2P
- cilj je minimizirati signalizacijski promet
- pristupne tehnologije:
 - IEEE 802.15.4 (WPAN)
 - IEEE 802.15.1 (Bluetooth)
 - LoRa i Sigfox
 - IEEE 802.11ah (Wi-Fi)

6LoWPAN

- protokol za prijenos IPv6 paketa preko bežičnih mreža s niskom potrošnjom
- koristi se za smanjenje veličine IPv6 paketa i smanjenje potrošnje energije kod prijenosa paketa
- koristi se za povezivanje uređaja u IPv6 mrežu
- mehanizmi prilagodbe:
 - **Kompresija zaglavlja**

- 6LoWPAN omogućuje komprimiranje IPv6 zaglavlja, čime se smanjuje veličina paketa i štedi se protok
- polja u zaglavlju IPv6 se odbacuju kada ih sloj prilagodbe može zaključiti iz okvira 802.15.4
- izostavljaju se standardna zaglavlja i pretpostavljaju opće korištene vrijednosti
- **Fragmentacija paketa**
 - 6LoWPAN omogućuje razbijanje IPv6 paketa na manje dijelove, kako bi se omogućilo prijenos paketa koji su veći od maksimalne veličine koju podržava IEEE 802.15.4 protokol
 - fragmenti ne moraju stići ispravnim redoslijedom, ali moraju unutar 60 s
- **Mesh-adresiranje**
 - 6LoWPAN koristi skraćeno adresiranje za IPv6 adrese u mrežama koje koriste IEEE 802.15.4 protokol, čime se štedi prostor u paketima

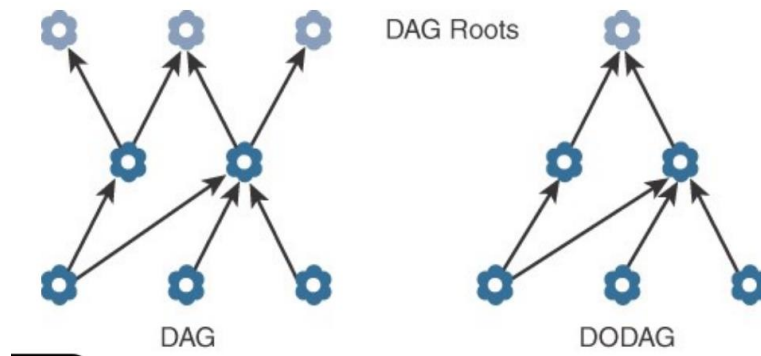
6TiSCH

- temelji se na IEEE 802.15.4e protokolu i koristi slojeviti pristup kako bi se omogućila optimalna mrežna povezanost i resursna upravljanje u mrežama s velikim brojem IoT uređaja
- namijenjen je korištenju u industrijskim i komercijalnim okruženjima
- temelji se na Time Slotted Channel Hopping (TSCH) modu koji omogućuje strog raspored vremenskih režnjeva za bežični prijenos podataka
- **6top**
 - omogućuje višim slojevima upravljanje nad IEEE 802.15.4e uređajima
 - Potrebno je sinkronizirati slanje i primanje okvira pomoću posebnog scheduling algoritma koji definira kako se koriste vremenski odsjecci
 - scheduling utječe na propusnost, kašnjenje i potrošnju energije
- **6TiSCH schedule management mehanizmi**
 - **Statični** – svi čvorovi u mreži dijele statični raspored ćelija
 - **Neighbour-to-neighbour** – definira se raspored na temelju opažanja komunikacije između čvorova

RPL

- protokol usmjeravanja za mreže s niskom potrošnjom energije i gubitke paketa
- koristi hijerarhijski pristup usmjeravanja i koristi topologiju stabla za povezivanje uređaja u mreži
- izgrađuje se posebno stablo (DODAG) koristeći kontrolne poruke koje prenosi protokol Internet Control Message Protocol (ICMPv6)
- 2 načina rada:
 - **Storing mode**
 - svi čvorovi održavaju potpunu tablicu usmjeravanja za jednu RPL domenu

- svaki čvor zna odrediti put prema svim ostalim čvorovima u podmreži RPL
- **Non-storing mode**
 - samo rubni usmjeritelj RPL domene sadrži potpunu tablicu usmjeravanja i zna odrediti put do krajnjeg čvora
 - svi ostali čvorovi održavaju samo listu roditelja za usmjeravanje prema rubnom usmjeritelju
- **DAG (Directed Acyclic Graph)**
 - usmjereni graf bez usmjerenih petlji, poruka se u DAG-u ne može vratiti do čvora koji je izvorno generira
- **DODAG (Destination-Oriented DAG)**
 - DAG s jednim korijenskim čvorom
 - svaki čvor održava do tri roditelja koji osiguravaju put do korijena
 - korijenski čvor za RPL zapravo je rubni usmjeritelj



- Vrste čvorova:
 - **DODAG root**
 - korijenski čvor, zadužen za inicijalizaciju topologije, održava stanje o topologiji DODAG
 - to je zapravo rubni usmjeritelj
 - **RPL Router Node**
 - uređaj koji može generirati i usmjeravati RPL pakete
 - **RPL Leaf Node**
 - uređaj na dnu topologije i usmjerava samo vlastite pakete prema čvoru roditelju
- Kontrolne poruke RPL-a
 - **DODAG Information Solicitation (DIS)**
 - čvor šalje svojim susjedima kada od njih zahtijeva informaciju o usmjeravanju tj. DODAG Information Object (DIO)
 - **DODAG Information Object (DIO)**
 - odgovor na poruku DIS, sadrži informaciju o roditelju i rang u DODAG-u
 - čvor je koristi kako bi održavao informaciju o DODAG-u u kojem se nalazi, a može biti član i većeg broja DODAG-a

- **Destination Advertisement Object (DAO)**
 - omogućuje propagaciju informacije o svakom pojedinom čvoru prema korijenskom čvoru